The Extension

Volume 4•Issue 3

MAY–JUNE 2003

A Technical Supplement to Control Network

Introduction to SNMP

By George Thomas, Contemporary Controls

INTRODUCTION

One of the numerous acronyms from the Internet world is SNMP which stands for Simple Network Management Protocol. Of course, anything termed "simple" is suspect. SNMP is an Internet protocol for managing devices on IP networks. Usually people think SNMP only applies to managed Ethernet switches, but it can be applied to any device that supports IP or TCP protocols. This includes printers, workstations, servers, modems and even industrial I/O devices. SNMP introduces us to the concept of "managed" devices which offers numerous advantages over unmanaged devices and could prove beneficial in industrial applications. As more and more devices embrace Ethernet, adding SNMP support can lead to greater advantages.

SNMP Versions

When we say a device is managed, we mean the device supports the SNMP protocol beyond its normal functions. The SNMP protocol, described in RFC 1157, was developed in the 80s as a simple means of accessing devices remotely. Originally intended to manage routers, SNMP can be used to manage any device including programmable logic controllers and remote I/O blocks. The example that is usually given refers to its use in monitoring the temperature inside a router. If this can be done, then there are a host of industrial applications limited only by our imagination.

One would think there is only one version of SNMP since this acronym is frequently quoted as if it is understood by all. Actually, there are three. The first is SNMPv1 which remains the most popular version. SNMPv2 builds upon the commands of version 1. SNMPv3 addresses the biggest criticism of SNMP. The commands are sent in clear-text and, therefore, insecure. SNMPv3 adds cryptography. Simply understanding SNMPv1 is enough to learn the concepts.

SNMP is an application layer protocol that sits above the TCP/IP stack. However, SNMP does not use TCP at all. It uses the UDP (datagram) protocol for communication which provides no acknowledgement that a transmission was successful. This was done to minimize the software requirements in the "agent" which is the device being managed. The "manager" is the device requesting information from the agent and it is called a Network Management Station (NMS). The interaction between a manager and an agent is similar to the interaction between a master and a slave device. The manager can initiate a "poll" of the agent requesting information or directing an action. The agent, in turn, generates a response to the query from the manager. This is how a remote I/O protocol works. However, the manager can request that a "trap" be set by the agent. A trap is simply a report to be issued in the future which is triggered when a set of conditions are met, similar to an alarm. The trap is triggered upon an event and once it occurs, the agent immediately reports the occurrence without a poll from the manager. This is no different from having a remote I/O device report on a "change of state." The NMS that receives the trap can then take appropriate action such as notifying personnel of the event. In this situation, the NMS is acting as a server by gathering data from agents and providing information on the state of devices to clients.

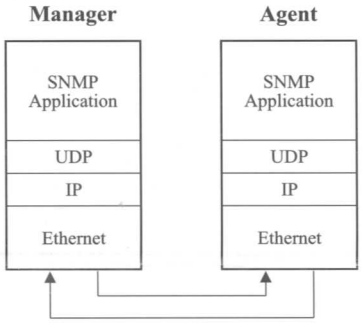

FIG. 1 - SNMP Communication occurs between a manager and agent by means of UDP datagrams.

Let's consider a real-world example. We have a remote pumping station with a SCADA system attached to several devices. The SCADA system is powered from an uninterruptible power supply (UPS) that has an SNMP agent. An Ethernet fiber optic link is used for communication between the remote pumping station and the main control room. An Ethernet switch, located in the pump house, connects the UPS and the SCADA system to the Ethernet link. An SNMP manager application, running on a desktop workstation located in the main control room and functioning as a NMS, instructs the agent in the pump house UPS to set a trap that will be triggered if there's a loss of main power. If this condition occurs, the agent would send a trap message back to the NMS which, in turn, pages the maintenance shop. This is a simple case in point of how SNMP can aid applications in our industry.

The beauty of SNMP is that it is indeed straightforward. There are only five commands with SNMPv1 and a total of nine for SNMPv2 and SNMPv3. The commands for SNMPv1 are listed below:

- get
- get-next
- set
- get-response
- trap

The additional commands for SNMPv2 and SNMPv3 are as follows:

- get bulk
- notification
- inform
- report

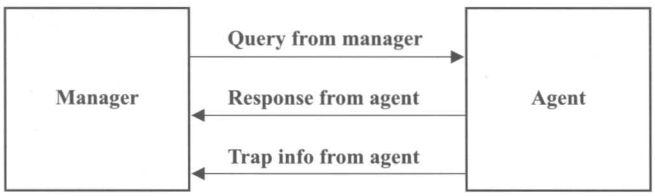

FIG. 2- A manager polls an agent in a similar fashion to a master/slave protocol.

To understand how the commands are applied, we need to introduce an integral component in the process: the managed objects that reside in the agent.

MANAGED OBJECTS

Each agent consists of a collection of managed objects that explain the capabilities and behavior of the agent in an abstract form. This is no different from the method by which a DeviceNet device is described by a collection of objects. The objects supported by a DeviceNet limit switch differ from that of a DeviceNet pneumatic manifold block; however, all DeviceNet devices support some common objects. This is the same situation with agents. All SNMP agents must support a common set of managed objects, called a Management Information Base (MIB). But an agent must support, at a minimum, what is defined in RFC 1213: MIB-2.

You might ask what happened to MIB-1? In the ever-changing Internet world, MIB-2 superseded MIB-1. Before we examine the details of MIB-2, we need to understand the structure and naming convention of MIBs. The Structure of Management Information (SMI) is described in RFC 1155. First, we will study the naming convention for managed objects and the MIBs themselves, which are simply a collection of managed objects. The term to identify an object is simply the Object ID (OID).

OBJECT ID

Managed objects within an agent are organized into a tree-like hierarchy similar to the way files and folders are used to represent the contents of a hard disk. In fact, some NMS software displays the management objects in a graphical fashion as if they were indeed files. However, the nomenclature is different. Managed objects are identified as a series of integers separated by dots representing the nodes on a tree. Naming begins at the root, followed by branches and ending in leaves. Let me give an example. In FIG. 3 you will see the tree structure for finding MIB-2. It begins at the root on the left. There are three branches, but we are interested only in iso(1). From iso(1) we have three more branches, but we are only interested in org(3). Next there are six more branches, but we follow dod(6). From this branch we go to internet(1). At this node we are at the base of all SNMP MIBs. The short form for representing where we are is 1.3.6.1 or we could say iso.org.dod.internet.

At this point we could follow either mgmt(2) or private(4) branches. If we follow the mgmt(2) branch, we will find standard MIBs. If we follow the private(4) branch, we will find vendor-specific MIBs. This is where a vendor can register unique products with corresponding unique management information. For example, a UPS would have much different information to share than an Ethernet switch. We will follow the mgmt branch and locate MIB-2 which is at 1.3.6.1.2.1 or you could simply say mgmt(1) which uniquely identifies its location.

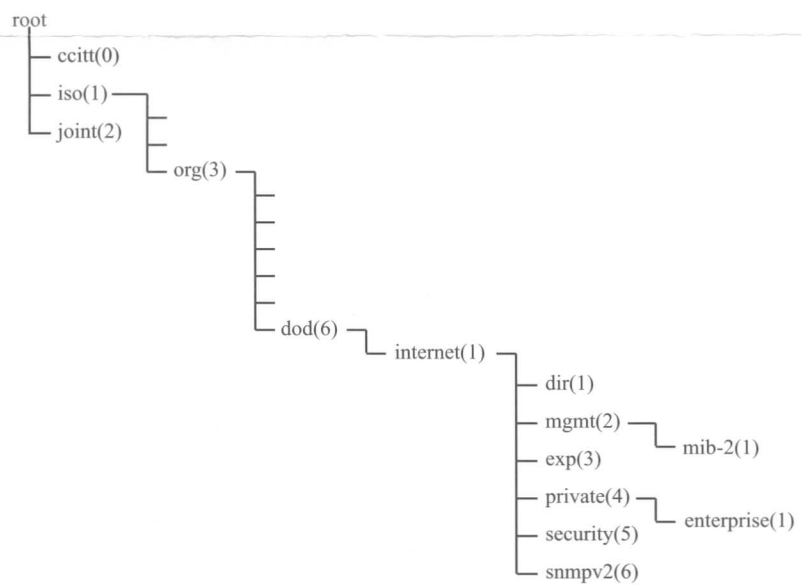

FIG. 3- The identification of objects follows a hierarchical structure.

We have found MIB-2, but we do not know the location of the individual managed objects. It's best to remember that MIB-2 is a collection of objects and each object description is identified in RFC 1213. If we study RFC 1213, we will learn there are ten managed object groups in MIB-2 as explained on page 3.

The first object group is system. The system group lets you enter the physical location of the device, the name of the device and who is responsible for the device. Therefore, if the device is queried by a management system, it could say it was tagged UPS-1, located in the pump house and if there is trouble to call Randy in the Instrument Shop. Another attribute of this object is up-time. It will continue to accumulate time until it is unpowered.

The 10 Managed Object Groups in MIB-2

mib-2	1	system	; General information about device for administrative purposes
mib-2	2	interfaces	; Keeps track of each interface on device
mib-2	3	at	; Address translation (only for backward compatibility)
mib-2	4	ip	; Tracks IP (Internet Protocol) aspects
mib-2	5	icmp	; Tracks ICMP (Internet Control Message Protocol) aspects
mib-2	6	tcp	; Tracks TCP (Transmission Control Protocol) aspects
mib-2	7	udp	; Tracks UDP (User Datagram Protocol) aspects
mib-2	8	egp	; Tracks EGP (Exterior Gateway Protocol) aspects
mib-2	9	(no longer used)	
mib-2	10	transmission	; Currently not used
mib-2	11	snmp	; Tracks SNMP (Simple Network Management Protocol) aspects

SETTING TRAPS

As mentioned before, a trap is an exception report similar to a change-of-state response from an I/O device. The manager establishes the trap in an agent. The agent monitors the situation and only reports to the manager if the trap is tripped. There are seven generic traps, but one is reserved for vendors for their specific application. The traps are as follows:

Generic Trap

Name, Number and Definition

coldStart (0)

Indicates that the agent has rebooted. All management variables will be reset; specifically, Counters and Gauges will be reset to zero (0). When a device is powered on, it sends this trap to its trap destination.

warmStart (1)

Indicates that the agent has reinitialized itself. None of the management variables will be reset.

linkDown (2)

Sent when an interface on a device goes down and identifies which interface.

linkUp (3)

Sent when an interface on a device comes back up and identifies which interface.

authenicationFailure(4)

Indicates that someone has tried to query the agent with an incorrect password.

egpNeighborLoss (5)

Indicates that an Exterior Gateway Protocol (EGP) neighbor has gone down.

enterpriseSpecific (6)

Indicates that the trap is vendor specific.

As seen from this list, a much simpler approach can be taken to monitoring a device in the field besides polling. For example, a coldstart could indicate some unauthorized activity in the field that triggered the trap. The use of traps is no different from having the benefit of a remote annunciator in the field but without the added expense. By studying the vendor specific traps that are available from a particular product, more ingenious reporting is possible.

CONFIGURATION

Before commissioning a managed device in the field, its agent must be configured. This is not unlike the commissioning needed before installing a DeviceNet limit switch or photoeye. With DeviceNet, you would use some tool or a program running on a laptop PC. Some devices will have a serial port that will support an ASCII terminal. If a terminal is unavailable, you could run a terminal emulation program on a PC. The advantage of this approach is that your network does not need to be up in order to commission the device. The second approach is to run a Telnet session over Ethernet. Of course, to do this the device must have its IP address already assigned. The screen on the PC will look the same but the network needs to be running. However, you could commission the device remotely from the control room with Telnet. In both of these cases, text screens are provided and the operator simply needs to fill in the blanks. The third approach is to use a web browser. This assumes that the managed device will serve up a web page for commissioning. With web technology, the screens are more colorful and data input is not restricted to simple command lines. Any of these approaches is possible but what data must be entered?

There are several parameters that must be set in the agent. The agent will consume an IP address for it to function as a management port. You might want to name the device, indicate its physical location and identify the person responsible for the device. You can even append a password to protect your settings. If traps are to be used, you need to identify the IP addresses of the managers that will receive the traps. There is usually space to list several IP addresses. What is significant here is that you need to know all this information before commissioning and to be careful not to reassign the master IP addresses, otherwise the traps will fail to find a manager. It would be a good idea to document all these parameters so a replacement device can be properly configured before putting the unit into service.

MANAGERS

Most of the discussion has been about agents and little about network management software. Command line programs can be used to poll agents and view responses, but the process is tedious since the operator needs to fully understand the structure of MIBs and each object's syntax. There are several commercial software packages and some freeware packages that will poll agents, set traps and receive and display trap responses while providing a more convenient user interface. Since SNMP was developed before the Worldwide Web protocols were developed, much of the data that is displayed is text-based. Later versions of network management software take advantage of Windows functionality and provide more versatility such as trending. It will take an operator some time to learn the intricacies of

the program but from one workstation, an operator can view all SNMP compatible devices.

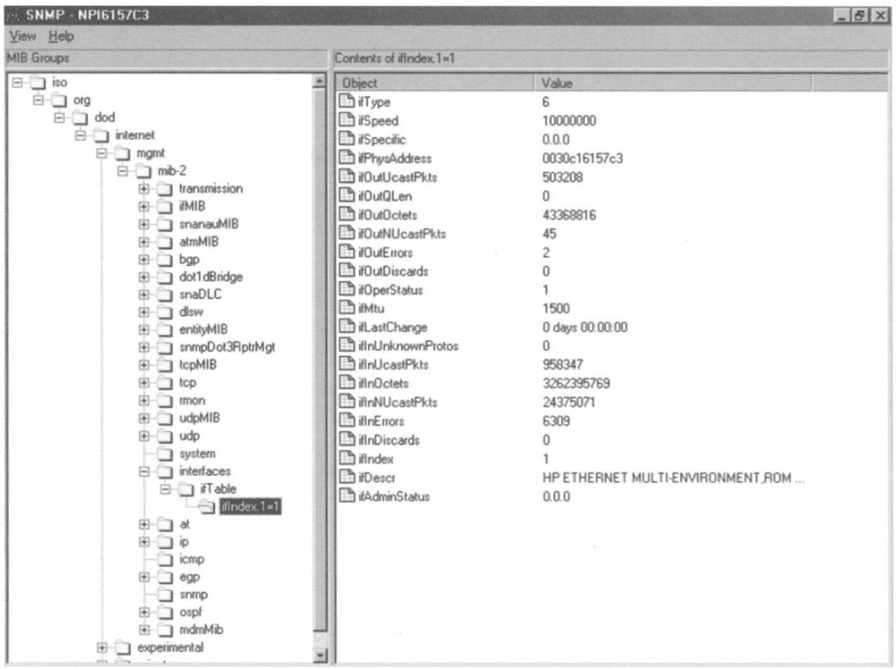

FIG. 4 - Typical manager screen.

With increasing interest in making a web browser the default operator interface for a system, can SNMP data be displayed on a browser screen? Some newer managed devices have built-in web servers that can serve up SNMP data. The advantage of a built-in web server is that it provides a convenient method of configuring the device and, an opportunity to verify that the device is functioning by being able to access it from the web. The other advantage is that the managed device with its internal web server can operate stand-alone without the need for any network management software. The trick comes in when several managed devices are to be viewed from one browser. There is no consistency of data presentation from the various vendors of web-based managed devices. It is also inconvenient to remember all the various URLs that must be selected to view the individual managed devices.

For our industry, there is another approach. It is possible to have an OPC server running in the manager that understands the SNMP protocol and can query MIB data, but display the data in a format comfortable to the operator. If the operator is viewing a process automation screen to view instruments and controllers and alarms, the information from managed devices can be included within the same screen; thus, making for a neat uniform appearance. The operator does not need to run a totally different application program to monitor the health of the network. There are several vendors in our industry that provide such a product.

CONCLUSION

With more and more devices embracing Ethernet and Internet protocols, the addition of SNMP protocol support adds benefits to the device. Managed devices support the SNMP protocol and are called agents. Agents consist of a collection of managed objects that can be queried by a manager to determine the health of the network or the status of particular devices. By displaying this data in an easily understood format, operators and maintenance personnel, located at a central site, can monitor the performance of the entire network by observing selected devices and pinpointing potential problems before they occur. Although commercial and freeware network management software programs exist for this purpose, the trend is to use more web-based tools. SNMP is not restricted to just the management of switches and routers. Any industrial device can have SNMP support and could provide much aid in industrial applications.

REFERENCES

Mauro, Douglas R. & Schmidt, Kevin J., Essential SNMP, O'Reilly & Associates, Inc., 2001.

Open DeviceNet Vendors Association, DeviceNet Specifications, Volume 1, Release 2.0, 1995.

Internet Engineering Task Force, RFC 1157—A Simple Network Management Protocol (SNMP), 1990.

Internet Engineering Task Force, RFC 1213—Management Information Base II, 1990.